



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/852,937	05/10/2001	David M. Blaker	9269-5	5828

20792 7590 05/31/2006

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER

LANIER, BENJAMIN E

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 05/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/852,937	Applicant(s) BLAKER ET AL.	
	Examiner Benjamin E Lanier	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 April 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3,6,16-18,21,27-29 and 32 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3,6,16-18,21,27-29 and 32 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 10 May 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 28 April 2006 has been entered.

Response to Amendment

2. The amendment filed 28 April 2006 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: the local memory is exclusively associated with the cryptographic processor. Page 13 of the specification on lines 7-8 recites "a load command loads one or more operands from the system memory 22 (e.g., the data buffer(s) 47) to the local memory 36 at block 142," which shows that the local memory is not exclusively associated with the cryptographic processor.

Applicant is required to cancel the new matter in the reply to this Office Action.

Response to Arguments

3. Applicant's arguments, filed 28 April 2006, that England does not disclose a local memory that is exclusively associated with a cryptographic processor have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Davis, U.S. Patent No. 5,844,986.

Claim Rejections - 35 USC § 101

4. Claims 27-29, 32 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 27-29, 32 are directed to a computer program product that comprises a computer readable program medium having computer readable program code embodied therein. The specification discloses that this computer readable medium can be electromagnetic, infrared (Page 6), and even a sheet of paper with code printed thereon (Page 7). These claims are nonstatutory because the mediums described in the specification are not capable of causing functional change in a computer. See, e.g., Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760. “Functional descriptive material consists of data structures and computer programs which impart functionality when employed as a computer component.” Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility Annex IV, Oct. 26, 2005, at http://www.uspto.gov/web/offices/pac/dapp/opla/preognotice/guidelines101_20051026.pdf, 1300 OG 142 (Nov. 22, 2005). The claims should be amended to specify that the computer readable program medium is a storage medium.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 1, 6, 16, 21, 27, 32 and rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the

Art Unit: 2132

relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The added material which is not supported by the original disclosure is as follows: the local memory is exclusively associated with the cryptographic processor. Page 13 of the specification on lines 7-8 recites “a load command loads one or more operands from the system memory 22 (e.g., the data buffer(s) 47) to the local memory 36 at block 142,” which shows that the local memory is not exclusively associated with the cryptographic processor. For the purposes of examination it will be assumed that the local memory is intended to be an element of the cryptographic processor as shown in figure 1 of the specification.

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1, 2, 16, 17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

9. Claim 1 recites, “generating a result...storing the result at a second relative position in the location memory,” and claim 2 recites, “executing the instruction that references...a second one of the operands using a second relative position in the local memory,” which renders the claim indefinite because it is unclear whether the claimed result or the second operand is stored at the second position in local memory. For the purposes of examination, the claims will be treated as having the claimed first and second operands being reference from contiguous locations in location memory with the result of the instruction being stored in a non-specific location of the local memory.

Art Unit: 2132

10. Claim 16 recites, “generating a result...storing the result at a second relative position in the location memory,” and claim 17 recites, “executing the instruction that references...a second one of the operands using a second relative position in the local memory,” which renders the claim indefinite because it is unclear whether the claimed result or the second operand is stored at the second position in local memory. For the purposes of examination, the claims will be treated as having the claimed first and second operands being reference from contiguous locations in location memory with the result of the instruction being stored in a non-specific location of the local memory.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

12. Claims 1, 6, 16, 21, 27, 32 are rejected under 35 U.S.C. 102(b) as being anticipated by Davis, U.S. Patent No. 5,844,986. Referring to claim 1, Davis discloses a secure bios system that includes a host processor coupled to system memory (Figure 1, elements 30 & 32) and a cryptographic processor coupled to a local memory (Figure 1, elements 41 & 42), which meets the limitations of a cryptographic processing system that comprises a host processor, a system memory coupled to the host processor, a cryptographic processor integrated circuit that comprises a local memory and is coupled to the host processor and the system memory (Figure 1, element 33), the local memory is exclusively associated with the cryptographic processor. The cryptographic processor actively retrieves new BIOS program code from the host processor

Art Unit: 2132

system memory, and stores the new BIOS program internally (Col. 3, lines 54-58), which meets the limitation of loading at least one operand from the system memory to the local memory. The cryptographic processor authenticates the new BIOS program code using digital signature techniques that require public/private key cryptography (Col. 3, line 65 – Col. 4, line 4), which meets the limitation of executing an instruction using the cryptographic processor that references the at least one operand using a first relative position in the local memory. The digital signature generated would meet the limitation of a result generated based on the at least one operand. Once the authentication operations have been performed, the cryptographic processor can make a determination as to the validity of the new BIOS program (Col. 4, lines 7-10). Since this determination is being performed in the cryptographic processor, the digital signature would have to be stored in the local memory so that the cryptographic processor could operate on it when making the determination. Therefore, the limitation of storing the result at a second relative position in the local memory is met. Whenever data is stored, it is stored in a position relative to the base address of that local memory, and that position can be measured by an offset from that base address. Therefore, the limitation of the first relative position comprises a first offset from a base address in the local memory, and the second relative position comprises a second offset from the base address in the local memory.

Referring to claim 6, Davis discloses a secure bios system that includes a host processor coupled to system memory (Figure 1, elements 30 & 32) and a cryptographic processor coupled to a local memory (Figure 1, elements 41 & 42), which meets the limitations of a cryptographic accelerator processor integrated circuit that comprises a local memory that is exclusively associated with the cryptographic accelerator processor. The cryptographic processor actively

Art Unit: 2132

retrieves new BIOS program code from the host processor system memory, and stores the new BIOS program internally (Col. 3, lines 54-58). The cryptographic processor authenticates the new BIOS program code using digital signature techniques that require public/private key cryptography (Col. 3, line 65 – Col. 4, line 4), which meets the limitation of executing an instruction using the cryptographic accelerator processor that references at least one operand using a first relative position in the local memory. The digital signature generated would meet the limitation of a result generated based on the at least one operand. Once the authentication operations have been performed, the cryptographic processor can make a determination as to the validity of the new BIOS program (Col. 4, lines 7-10). Since this determination is being performed in the cryptographic processor, the digital signature would have to be stored in the local memory so that the cryptographic processor could operate on it when making the determination. Therefore, the limitation of storing the result at a second relative position in the local memory is met. Whenever data is stored, it is stored in a position relative to the base address of that local memory, and that position can be measured by an offset from that base address. Therefore, the limitation of the first relative position comprises a first offset from a base address in the local memory, and the second relative position comprises a second offset from the base address in the local memory.

Referring to claim 16, Davis discloses a secure bios system that includes a host processor coupled to system memory (Figure 1, elements 30 & 32) and a cryptographic processor coupled to a local memory (Figure 1, elements 41 & 42), which meets the limitations of a cryptographic processing system that comprises a host processor, a system memory coupled to the host processor, a cryptographic processor integrated circuit that comprises a local memory and is

Art Unit: 2132

coupled to the host processor and the system memory (Figure 1, element 33), the local memory is exclusively associated with the cryptographic processor. The cryptographic processor actively retrieves new BIOS program code from the host processor system memory, and stores the new BIOS program internally (Col. 3, lines 54-58), which meets the limitation of means for loading at least one operand from the system memory to the local memory. The cryptographic processor authenticates the new BIOS program code using digital signature techniques that require public/private key cryptography (Col. 3, line 65 – Col. 4, line 4), which meets the limitation of means for executing an instruction using the cryptographic processor that references the at least one operand using a first relative position in the local memory. The digital signature generated would meet the limitation of means for generating a result based on the at least one operand. Once the authentication operations have been performed, the cryptographic processor can make a determination as to the validity of the new BIOS program (Col. 4, lines 7-10). Since this determination is being performed in the cryptographic processor, the digital signature would have to be stored in the local memory so that the cryptographic processor could operate on it when making the determination. Therefore, the limitation of means for storing the result at a second relative position in the local memory is met. Whenever data is stored, it is stored in a position relative to the base address of that local memory, and that position can be measured by an offset from that base address. Therefore, the limitation of the first relative position comprises a first offset from a base address in the local memory, and the second relative position comprises a second offset from the base address in the local memory.

Referring to claim 21, Davis discloses a secure bios system that includes a host processor coupled to system memory (Figure 1, elements 30 & 32) and a cryptographic processor coupled

Art Unit: 2132

to a local memory (Figure 1, elements 41 & 42), which meets the limitations of a cryptographic accelerator processor integrated circuit that comprises a local memory that is exclusively associated with the cryptographic accelerator processor. The cryptographic processor actively retrieves new BIOS program code from the host processor system memory, and stores the new BIOS program internally (Col. 3, lines 54-58). The cryptographic processor authenticates the new BIOS program code using digital signature techniques that require public/private key cryptography (Col. 3, line 65 – Col. 4, line 4), which meets the limitation of means for executing an instruction using the cryptographic accelerator processor that references at least one operand using a first relative position in the local memory. The digital signature generated would meet the limitation of a means for generating a result based on the at least one operand. Once the authentication operations have been performed, the cryptographic processor can make a determination as to the validity of the new BIOS program (Col. 4, lines 7-10). Since this determination is being performed in the cryptographic processor, the digital signature would have to be stored in the local memory so that the cryptographic processor could operate on it when making the determination. Therefore, the limitation of means for storing the result at a second relative position in the local memory is met. Whenever data is stored, it is stored in a position relative to the base address of that local memory, and that position can be measured by an offset from that base address. Therefore, the limitation of the first relative position comprises a first offset from a base address in the local memory, and the second relative position comprises a second offset from the base address in the local memory.

Referring to claim 27, Davis discloses a secure bios system that includes a host processor coupled to system memory (Figure 1, elements 30 & 32) and a cryptographic processor coupled

Art Unit: 2132

to a local memory (Figure 1, elements 41 & 42), which meets the limitations of a cryptographic processing system that comprises a host processor, a system memory coupled to the host processor, a cryptographic processor integrated circuit that comprises a local memory and is coupled to the host processor and the system memory (Figure 1, element 33), the local memory is exclusively associated with the cryptographic processor, a computer readable program medium having computer readable program code embodied therein. The cryptographic processor actively retrieves new BIOS program code from the host processor system memory, and stores the new BIOS program internally (Col. 3, lines 54-58), which meets the limitation of computer readable program code for loading at least one operand from the system memory to the local memory. The cryptographic processor authenticates the new BIOS program code using digital signature techniques that require public/private key cryptography (Col. 3, line 65 – Col. 4, line 4), which meets the limitation of computer readable program code for executing an instruction using the cryptographic processor that references the at least one operand using a first relative position in the local memory. The digital signature generated would meet the limitation of computer readable program code for generating a result based on the at least one operand. Once the authentication operations have been performed, the cryptographic processor can make a determination as to the validity of the new BIOS program (Col. 4, lines 7-10). Since this determination is being performed in the cryptographic processor, the digital signature would have to be stored in the local memory so that the cryptographic processor could operate on it when making the determination. Therefore, the limitation of computer readable program code for storing the result at a second relative position in the local memory is met. Whenever data is stored, it is stored in a position relative to the base address of that local memory, and that

position can be measured by an offset from that base address. Therefore, the limitation of the first relative position comprises a first offset from a base address in the local memory, and the second relative position comprises a second offset from the base address in the local memory.

Referring to claim 32, Davis discloses a secure bios system that includes a host processor coupled to system memory (Figure 1, elements 30 & 32) and a cryptographic processor coupled to a local memory (Figure 1, elements 41 & 42), which meets the limitations of a cryptographic accelerator processor integrated circuit that comprises a local memory that is exclusively associated with the cryptographic accelerator processor, computer readable program medium having computer readable program code embodied therein. The cryptographic processor actively retrieves new BIOS program code from the host processor system memory, and stores the new BIOS program internally (Col. 3, lines 54-58). The cryptographic processor authenticates the new BIOS program code using digital signature techniques that require public/private key cryptography (Col. 3, line 65 – Col. 4, line 4), which meets the limitation of computer readable program code for executing an instruction using the cryptographic accelerator processor that references at least one operand using a first relative position in the local memory. The digital signature generated would meet the limitation of a computer readable program code for generating a result based on the at least one operand. Once the authentication operations have been performed, the cryptographic processor can make a determination as to the validity of the new BIOS program (Col. 4, lines 7-10). Since this determination is being performed in the cryptographic processor, the digital signature would have to be stored in the local memory so that the cryptographic processor could operate on it when making the determination. Therefore, the limitation of computer readable program code for storing the result at a second relative

Art Unit: 2132

position in the local memory is met. Whenever data is stored, it is stored in a position relative to the base address of that local memory, and that position can be measured by an offset from that base address. Therefore, the limitation of the first relative position comprises a first offset from a base address in the local memory, and the second relative position comprises a second offset from the base address in the local memory.

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

14. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

15. Claims 2, 17, 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, U.S. Patent No. 5,844,986, in view of Garger, U.S. Patent No. 6,029,170. Referring to claim 2, Davis discloses a secure BIOS system wherein new BIOS code is digital signed in a cryptographic processor using public/private key cryptography (Col. 3, line 65 – Col. 4, line 4). The key used to the digitally sign the code can be retrieved from the host processor memory to the cryptographic processor memory (Col. 4, lines 47-56), which meets the limitation of loading

at least two operands from the system memory to local memory. Davis does not disclose that the new BIOS code and the key used to digitally sign the code are stored contiguously within the local memory of the cryptographic processor. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the new BIOS code and the key used to sign the code to be stored contiguously in the local memory of the cryptographic processor in order to maximize the data retrieval performance from the memory as taught in Ganger (Col. 7, lines 11-13), which would ultimately cut down on processing time.

Referring to claim 17, Davis discloses a secure BIOS system wherein new BIOS code is digital signed in a cryptographic processor using public/private key cryptography (Col. 3, line 65 – Col. 4, line 4). The key used to the digitally sign the code can be retrieved from the host processor memory to the cryptographic processor memory (Col. 4, lines 47-56), which meets the limitation of loading at least two operands from the system memory to local memory. Davis does not disclose that the new BIOS code and the key used to digitally sign the code are stored contiguously within the local memory of the cryptographic processor. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the new BIOS code and the key used to sign the code to be stored contiguously in the local memory of the cryptographic processor in order to maximize the data retrieval performance from the memory as taught in Ganger (Col. 7, lines 11-13), which would ultimately cut down on processing time.

Referring to claim 28, Davis discloses a secure BIOS system wherein new BIOS code is digital signed in a cryptographic processor using public/private key cryptography (Col. 3, line 65 – Col. 4, line 4). The key used to the digitally sign the code can be retrieved from the host processor memory to the cryptographic processor memory (Col. 4, lines 47-56), which meets the

Art Unit: 2132

limitation of loading at least two operands from the system memory to local memory Davis does not disclose that the new BIOS code and the key used to digitally sign the code are stored contiguously within the local memory of the cryptographic processor. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the new BIOS code and the key used to sign the code to be stored contiguously in the local memory of the cryptographic processor in order to maximize the data retrieval performance from the memory as taught in Ganger (Col. 7, lines 11-13), which would ultimately cut down on processing time.

16. Claims 3, 18, 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, U.S. Patent No. 5,844,986, in view of Garger, U.S. Patent No. 6,029,170 as applied to claims 1, 2, 16, 17, 27, 28 above, and further in view of Mahmoud, U.S. Patent No. 6,567,911, in view of Schneier. Referring to claim 3, Davis discloses a secure BIOS system wherein new BIOS code is digital signed in a cryptographic processor using public/private key cryptography (Col. 3, line 65 – Col. 4, line 4). Davis does not disclose that the BIOS code and the key used to digitally sign the code are different sizes. Mahmoud discloses that the typical BIOS is about 64k (Col. 1, lines 35-37). We know that a kilobyte is approximately 1,024 bytes, and that there are approximately 8 bits in a byte. Therefore, the typical BIOS would be approximately 524,288 bits in length.

Schneier discloses that the desired key length for various cryptographic operations of varying security is no more than 128 bits (Pages 166-167). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the BIOS code and the key used to digitally sign the code in the secure BIOS system of Davis to be different sizes because the cost paid in computing time to use a key of 500,000 bits in length does not justify what is being secured in Davis (See Schneier Pages 160-161), which is simply a BIOS.

Referring to claim 18, Davis discloses a secure BIOS system wherein new BIOS code is digital signed in a cryptographic processor using public/private key cryptography (Col. 3, line 65 – Col. 4, line 4). Davis does not disclose that the BIOS code and the key used to digitally sign the code are different sizes. Mahmoud discloses that the typical BIOS is about 64k (Col. 1, lines 35-37). We know that a kilobyte is approximately 1,024 bytes, and that there are approximately 8 bits in a byte. Therefore, the typical BIOS would be approximately 524,288 bits in length. Schneier discloses that the desired key length for various cryptographic operations of varying security is no more than 128 bits (Pages 166-167). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the BIOS code and the key used to digitally sign the code in the secure BIOS system of Davis to be different sizes because the cost paid in computing time to use a key of 500,000 bits in length does not justify what is being secured in Davis (See Schneier Pages 160-161), which is simply a BIOS.

Referring to claim 29, Davis discloses a secure BIOS system wherein new BIOS code is digital signed in a cryptographic processor using public/private key cryptography (Col. 3, line 65 – Col. 4, line 4). Davis does not disclose that the BIOS code and the key used to digitally sign the code are different sizes. Mahmoud discloses that the typical BIOS is about 64k (Col. 1, lines 35-37). We know that a kilobyte is approximately 1,024 bytes, and that there are approximately 8 bits in a byte. Therefore, the typical BIOS would be approximately 524,288 bits in length. Schneier discloses that the desired key length for various cryptographic operations of varying security is no more than 128 bits (Pages 166-167). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the BIOS code and the key used to digitally sign the code in the secure BIOS system of Davis to be different sizes because the cost paid in

Art Unit: 2132


computing time to use a key of 500,000 bits in length does not justify what is being secured in Davis (See Schneier Pages 160-161), which is simply a BIOS.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Benjamin E. Lanier